AMENDMENTS TO THE SPECIFICATION:

Please amend the specification as follows:

Please replace the paragraph appearing on page 1, lines 11-20, with the following paragraph:

The growth of the Internet has led to the development of numerous technologies for the distribution of content over the World Wide Web. Among these technologies are systems that permit Web content to include executable code[[,]] that is sent from a Web server to a Web client, where it is executed. Such "mobile code" or "applets" allow content providers to distribute content that includes programmed behavior, which may be used in a variety of ways. Mobile code systems, such as Java[[,]] (produced by Sun Microsystems[[,]] of Palo Alto, California), or Curl[[,]] (provided by Curl Corporation[[,]] of Cambridge, Massachusetts[[,]]) may greatly enhance the experience of Web users by providing a relatively efficient way for highly interactive or media-rich content to be sent across the Web.

Please replace the paragraph appearing on page 4, lines 18-20, with the following paragraph:

In view of the above, it would be desirable to provide a system and methods that permit mobile code to access resources on the Internet without exposing systems that execute the mobile code to a DNS spoofing attack.

Please replace the paragraph appearing on page 6, lines 25, through page 7, line11, with the following paragraph:

Referring to FIGS. 1A-1C, an example of a DNS spoofing attack on computers located behind a firewall is described. As seen in FIG. 1A, [[The]] the victim network for this attack, victim.com, has (at least) two computers located behind firewall 10. First victim computer 12 has, for example, a host name of dupe.victim.com, and has an IP address of 10.10.10.1. Second victim computer 14, which is the actual target of the attack, is named target.victim.com, and has an IP address of 10.10.10.2. Both of victim computers 12 and 14 access the Internet only through firewall 10, which prevents unauthorized network connections from computers outside of firewall 10 from being made with computers that are behind firewall 10. First victim computer 12 is operated by a user, who may use first victim computer 12 to connect to web sites that are outside of firewall 10. Second victim computer 14, which is the target of the attack, may contain valuable data, or may provide services that may cause harm if disrupted. Due to the value of the data stored on second victim computer 14, or the services it provides, second victim computer 14 is normally permitted to accept network connections only from trusted computers behind firewall 10, including first victim computer 12.

Please replace the paragraph appearing on page 14, lines 15-25, with the following paragraph:

In a preferred embodiment, the hostname file check and the connection between the applet and the other computer use the same IP address. For example, if the HTTP HEAD-request that is used to access URL 60 uses an IP address of 20.20.20.1 to access "www.example.com", then, when the applet creates a connection with "www.example.com", using an HTTP GET-request, for example, it uses the IP address 20.20.20.1. This restriction may be implemented by looking up the address of a computer to which a connection is being made using DNS, and then using that address to perform the HTTP HEAD-request, and to create any subsequent connection with the content server. This additional restriction prevents the address of the computer to which the connection is being made from changing between the hostname file check and the creation of the connection.

Please replace the paragraph appearing on page 17, lines 9-15, with the following paragraph:

At step 104, the network restriction software generates a URL for the hostname file in the name directory that must be checked before a network connection will be allowed. This is preferably done by using the host name of the computer with which the connection is to be made as the host name for the URL, and appending the pathname of the name directory[[,]] and the home site of the applet (i.e. the site from which the applet was downloaded), which corresponds in a preferred embodiment to the name of the hostname file.

Please replace the paragraph appearing on page 18, lines 3-10, with the following paragraph:

As seen in FIG. 7B, in accordance with the principles of the present invention, execution engine 77, which is running applet 72, attempts to access the URL "http://www.~~attacker~~target.victim.com/name-directory/www.attacker.com" on second victim computer 78. Since second victim computer 78 was not intended to respond to the name "www.attacker.com", the file "www.attacker.com" is not found in the name directory (if such a directory even exists on second victim computer 78), and execution engine 77 prevents applet 72 from creating a network connection with second victim computer 78, avoiding the attack.

Please replace the paragraph appearing on page 20, lines 3-13, with the following paragraph:

Referring now to FIG. 9, a block diagram of a computer system suitable for use with the present invention is described. Computer system 90 includes at least a processor 92 for processing information according to programmed instructions, and a memory 94, for storing information and instructions for processor 92. Additionally, computer system 90 may optionally include a storage system 96, such as a magnetic or optical disk system, for storing instructions and information on a relatively long-term basis. Computer system 90 also may include a network interface 97, and a display system 99, such as a video controller and monitor, on which information may be displayed. Processor 92, memory 94, storage system 96, network interface 97, and display system 99 are coupled to a bus 98, which preferably provides a high-speed means for devices connected to bus 98 to communicate with each other.